Privacy Notice

Below, we would like to provide you with an overview of the processing of your personal data in connection with this app.

1. Controller

The controller within the meaning of the General Data Protection Regulation and other national data protection laws of the Member States as well as other data protection provisions is:

Amprion GmbH

Robert-Schuman-Strasse 7

44263 Dortmund

Germany

E-mail: datenschutz@amprion.net

Fax: +49 231 5849 11139

For matters relating specifically to our app, please contact: mobileapp@amprion.net

2. Downloading the app

In connection with the download and installation of our app, we process:

- IP address
- date and time of the request
- access status/HTTP status code
- user's operating system
- volume of data transferred

The legal basis is our legitimate interest pursuant to Art. 6(1)(f) GDPR. Our legitimate interest consists in being able to provide you with our app. Please note, however, that, when the app is downloaded, the operator of the app store may also process information required for this purpose, such as your e-mail address, username and individual device identifier. We have no influence over the scope of this processing. The controller is the app store operator.

3. Creation of log files

Each time our app is accessed, temporary information transmitted by your end device to our servers is automatically stored. The log file created records the device type/version, the operating system used, the IP address and the date and time of the server request. The storage and processing of these data serve exclusively to provide you with the content of our app and to ensure system security. The legal basis for this is Art. 6(1)(f)

GDPR. Our legitimate interest consists in being able to provide you with our app and to secure the system.

4. Receipt of push notifications

The app provided by us has a function that allows push notifications to be sent to your end device. These include, for example, regular information about our services. When our app is installed, the operating system of your end device asks whether you wish to receive push notifications. If you activate push notifications, an installation ID is stored on your end device in order to deliver them to you and is read each time a notification is sent. The legal basis for this is Section 25(2) no. 2 TDDDG.

How to deactivate push notifications again:

Deactivation on an iOS end device:

1. Open “Settings” in your menu.
2. All apps are listed at the bottom. Scroll down until the name of our app is listed.
3. Tap the name of the app and then tap “Notifications”.
4. At this point, you may deactivate individual notification variants or push notifications completely.

Deactivation on an Android end device:

1. Pull down the notification shade at the top of the screen to open it. An overview of the most recent notifications will be displayed.
2. Tap and hold the relevant notification of the app for which you want to deactivate push notifications.
3. Either move the toggle to the other side so that you generally no longer receive notifications, or click “Details”. There you can select which notifications you wish to receive.

5. Cookies and similar technologies

Our app uses cookies and similar technologies (hereinafter “services”) to store information on your end device or to access information already stored on your end device. In some cases, this is strictly necessary to ensure the functionality and security of our app. Optionally, where you have given us your express consent, we also use third-party tracking technologies for analytics purposes. This enables us to continuously improve the user experience of our app.

a. Specifically, our app uses the following strictly necessary services:

aa. Firebase App Check

Firebase App Check accesses device attestation data that are stored on your end device by the app store operator when our app is downloaded. This enables us to rule out manipulation of our app and to ensure the security of the app. The legal basis for this is Section 25(2) no. 2 TDDDG in conjunction with Art. 6(1)(f) GDPR. Our legitimate interest consists in being able to provide you with our app and to secure our systems. Google Firebase App Check is a service of Google LLC, California, USA. The information generated by Firebase App Check is generally transmitted to a Google server in the USA and stored there. The legal basis for the transfer is a data processing agreement pursuant to Art. 28 GDPR, which we have concluded with Google. In addition, Google is certified under the so-called EU-U.S. Data Privacy Framework and is therefore deemed to be a recipient ensuring an adequate level of protection pursuant to Art. 45(1) GDPR.

bb. Firebase Remote Config

Firebase Remote Config enables us to carry out updates to our app without you having to download them separately. For this purpose, the service stores an installation ID on your end device when our app is installed. This ID is read each time the app is updated, which is strictly necessary in order to install the updates. The legal basis for this is Section 25(2) no. 2 TDDDG in conjunction with Art. 6(1)(f) GDPR. Our legitimate interest consists in being able to provide you with updates and security patches for our app. Google Firebase Remote Config is a service of Google LLC, California, USA. The information generated by Firebase Remote Config is generally transmitted to a Google server in the USA and stored there. The legal basis for the transfer is a data processing agreement pursuant to Art. 28 GDPR, which we have concluded with Google. In addition, Google is certified under the so-called EU-U.S. Data Privacy Framework and is therefore deemed to be a recipient ensuring an adequate level of protection pursuant to Art. 45(1) GDPR.

b. In addition, our app optionally uses the following analytics services:

aa. Firebase Crashlytics

Firebase Crashlytics stores a user ID on your end device, which, in the event of an app crash, is transmitted to us together with a crash report generated in real time. This enables us to better identify and resolve problems with our app. The legal basis for this is your consent pursuant to Section 25(1) TDDDG in conjunction with Art. 6(1)(a) GDPR. You may withdraw your consent at any time with effect for the future by opening and configuring the data protection settings accordingly. Firebase Crashlytics is a service of Google LLC, California, USA. The information generated by Firebase Crashlytics is generally transmitted to a Google server in the USA and stored there. The legal basis for the transfer is a data processing agreement pursuant to Art. 28 GDPR, which we have concluded with Google. In addition, Google is certified under the so-called EU-U.S. Data Privacy Framework and is therefore deemed to be a recipient ensuring an adequate level of protection pursuant to Art. 45(1) GDPR.

bb. Google Analytics for Firebase

Google Analytics is a web analytics service that enables us to analyse and better understand the use of our app. Information such as the IP address, number of users and sessions, session duration, operating systems, device models, region/geography, first launches and app opens is tracked. For this purpose, Google Analytics also accesses the storage of your end device. However, we use the code extension “anonymizeIP”. By using this extension, your IP address is truncated by Google within Member States of the European Union or in other Contracting States to the Agreement on the European Economic Area. Only in exceptional cases will the full IP address be transmitted to a server in the USA. However, anonymisation of the IP address does not mean that the processing as a whole is anonymised, as further usage data that qualify as personal data are collected when Google Analytics is used. For example, it may therefore be possible to link the data to the user of an existing Google account. The legal basis for this is your consent pursuant to Section 25(1) TDDDG in conjunction with Art. 6(1)(a) GDPR. You may withdraw your consent at any time with effect for the future by opening and configuring the data protection settings accordingly. The legal basis for the transfer to Google is a data processing agreement pursuant to Art. 28 GDPR, which we have concluded with Google. In addition, Google is certified under the so-called EU-U.S. Data Privacy Framework and is therefore deemed to be a recipient ensuring an adequate level of protection pursuant to Art. 45(1) GDPR.

5. Your rights as a data subject

Where personal data concerning you are processed, you are a data subject within the meaning of the GDPR and you have the rights described below towards us.

You may **request access** pursuant to Art. 15 GDPR to the personal data concerning you that we process. In your access request, you should specify your concern in order to make it easier for us to compile the required data.

If the information concerning you is not, or is no longer, accurate, you may request **rectification** pursuant to Art. 16 GDPR. If your data are incomplete, you may request that they be completed.

In General, we store your personal data only for as long as is necessary to achieve the respective purpose pursued by the data processing. Without prejudice to this, you may request the unscheduled **erasure** of your personal data under the conditions set out in Art. 17 GDPR.

Within the framework of the requirements of Art. 18 GDPR, you have the right to request **restriction** of the processing of the data concerning you.

Pursuant to Art. 21 GDPR, you have the right to **object**, on grounds relating to your particular situation, at any time to the processing of data concerning you.

To exercise your rights, please contact the controller named above, as your rights are also to be implemented there. You may also contact the Data Protection Officer directly, in particular where your concern requires a higher level of confidentiality:

The Data Protection Officer of Amprion

c/o migosens GmbH

Wiesenstr. 35

45473 Mülheim an der Ruhr

E-Mail: dsb-amprion@migosens.net

Tel: +49 (0) 208-99395110

Fax: +49 (0) 208-99395119

Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

Landesbeauftragte fuer Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Kavalleriestr. 2-4

40213 Duesseldorf

Germany

Telephone: 0211/38424-0

poststelle@ldi.nrw.de